



# Payment Card Industry Data Security Standard (PCI DSS)

**Does your organisation accept Visa, MasterCard, American Express, Discover, or JCB-branded credit or debit cards?** If so, your organisation is required to comply with the Payment Card Industry Data Security Standard. PwC has extensive experience assisting our clients with understanding their obligations, assessing the current state, and overseeing and assisting with compliance and remediation activities.

## Background

Organisations face a wide range of external and internal threats to confidential and proprietary data. In the wake of significant data compromises at Global Fortune 500 companies, the need to protect customer payment card data has advanced to the forefront. The Payment Card Industry Data Security Standard (PCI DSS) has been developed by the credit card industry to provide merchants and service providers with a common security framework to help ensure the confidentiality of payment card and associated customer data.

## What is the Payment Card Industry Data Security Standard?

The PCI standard is the result of a collaborative effort between the major credit card schemes to create common industry security requirements for the protection of cardholder data. The PCI standard consists of 6 categories, 12 requirements, approximately 200 controls and 250 individual testing procedures that focus on the confidentiality of payment card data:

### *Build and maintain a secure network*

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor supplied defaults for system passwords and other security parameters

### *Protect cardholder data*

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

### *Maintain a vulnerability management programme*

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

### *Implement strong access control measures*

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

### *Regularly monitor and test networks*

10. Track and monitor access to network resources and cardholder data
11. Regularly test security systems and processes

### *Maintain an information security policy*

12. Maintain a policy that addresses information security.

## Who does the PCI Standard apply to?

Compliance with the PCI standard is required for all entities that store, process or transmit credit or debit card data. Merchants that process more than one-million transactions ("Level 1" and "Level 2" merchants) and service providers are subject to the most stringent compliance validation requirements including an annual onsite security assessment and external vulnerability scans (by a certified assessor or Internal Audit department).

## When must organisations be compliant?

Although all of the card schemes' compliance dates have already passed, new compliance validation dates have been announced to encourage global PCI DSS compliance.

- Visa requires all Level 1 merchants to validate compliance by 30 September 2010.
- MasterCard requires all Level 1 and Level 2 merchants to validate compliance by 30 June 2011.

## What happens if my organisation is not compliant?

Organisations are contractually required to be compliant with the PCI DSS (through their contract with the card schemes or their acquiring bank). Failure to validate compliance on an annual basis may lead to fines, penalties, increased transaction costs, and potentially the inability to process credit cards.

In the US, Visa is fining Level 1 merchants \$25K per month and \$5K per month for Level 2 merchants. MasterCard is fining \$25K per month for Level 1 and Level 2 merchants and \$10K per month for Level 3. Fines are assessed to the merchant's acquiring bank and then passed on to the merchant.

## What are the common drivers for PCI compliance?

- Increased awareness and general concerns over data security and privacy
- Significant fines, penalties, and increased transaction processing costs
- Reputation and brand damage leading to loss of revenue
- Regulatory requirements around the privacy of customer data
- Industry peer pressure
- Alignment with corporate risk management guidelines
- Potential inability to process credit cards.

## What are the common mistakes organisations make?

- Viewing compliance as "an IT problem"
- Lacking a clear definition of the payment environment that is in scope for PCI certification
- Underestimating the extent and complexity of PCI compliance
- Not controlling logical access to systems containing payment card data
- Not consistently logging, monitoring, and responding to security events
- Not encrypting or protecting stored payment card data
- Not including PCI contractual language for third-party service providers
- Not planning and implementing scalable remediation solutions
- Taking a "siloes" approach to compliance.

## How have organisations reduced the scope and complexity of their PCI program?

- Network architecture redesign and segmentation
- Implementation of tokenisation and end-to-end encryption solutions
- Identification and elimination of unnecessary payment card data retention
- Payment application centralisation and consolidation
- Business process reengineering
- Payment processing outsourcing.

## Interesting Statistics from the US

- As of 30 September 2009, 97% of the Level 1 and 94% of the Level 2 merchants have validated compliance with PCI DSS.
- 99% of the Level 1 and Level 2 merchants have validated they do not retain prohibited data.
- Most companies were not compliant with at least 50% of the 200+ controls during their first assessment (even those with a mature security organisation).
- PCI remediation generally lasts between 6 to 24 months.

## How do I know my merchant tier level?

All merchants fall into one of the four merchant levels based on payment card transaction volume over a 12-month period. Transaction volume is based on the aggregate number of transactions (inclusive of card scheme branded credit, debit and prepaid cards) from a merchant Doing Business As ("DBA").

Tier	Criteria	Validation Requirements
1	<ul style="list-style-type: none"> <li>• Greater than 6m payment card transactions annually</li> <li>• Any company that has been compromised</li> <li>• Any business that has been classified as Level 1 by any other card scheme</li> </ul>	<ul style="list-style-type: none"> <li>• Annual on-site, data security assessment</li> <li>• Quarterly network scans</li> <li>• Annual external / internal penetration tests</li> </ul>
2	<ul style="list-style-type: none"> <li>• Between 1-6m payment card transactions per year</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Level 1</li> </ul>
3	<ul style="list-style-type: none"> <li>• Between 20K and 1m e-commerce payment card transactions per year</li> <li>• Merchants with &lt;50K payment card transactions (AMEX)</li> </ul>	<ul style="list-style-type: none"> <li>• Annual PCI self-assessment questionnaire</li> <li>• Quarterly network scans</li> <li>• Annual external / internal penetration tests</li> </ul>
4	<ul style="list-style-type: none"> <li>• Less than 20K e-commerce payment card transactions per year</li> <li>• Less than 1m traditional payment card transactions</li> </ul>	<ul style="list-style-type: none"> <li>• Same as Level 3</li> </ul>

## How do I know my service provider tier level?

Service providers are organisations that process, store, or transmit cardholder data on behalf of card scheme clients, merchants, or other service providers.

Tier	Criteria	Validation Requirements
1	<ul style="list-style-type: none"> <li>• All processors or any service provider that stores, processes and/or transmits over 300,000 payment card transactions annually</li> </ul>	<ul style="list-style-type: none"> <li>• Annual on-site PCI data security assessment</li> <li>• Annual external / internal penetration tests</li> <li>• Quarterly network scans</li> </ul>
2	<ul style="list-style-type: none"> <li>• Any service provider that stores, processes and/or transmits less than 300,000 payment card transactions annually</li> </ul>	<ul style="list-style-type: none"> <li>• Annual PCI self-assessment questionnaire</li> <li>• Annual external / internal penetration tests</li> <li>• Quarterly network scans</li> </ul>

## What is the cost of a payment card data breach?

- Fines and penalties ranging from \$5K - \$25K per month until PCI compliant
- \$500K fine per payment card data compromise incident if not PCI compliant
- \$100K fine if Visa is not immediately notified of a suspected data breach
- If track data or other sensitive data elements have been compromised, the merchant can be assessed the cost of fraud under Visa's Account Data Compromise Recovery (ADCR) Programme as well as cost of card reissuance
- Potential termination of credit card processing privileges
- Liability associated with fraud and losses
- Cost associated with brand damage and lost revenue
- Forensics assessment and containment
- IT and security remediation and enhancements
- PCI re-assessment and re-certification
- Potential class action lawsuits and liability.

## The PwC Point of View

There are many ways to achieve compliance with the PCI DSS. PricewaterhouseCoopers believes the most effective approach is to view PCI not as another compliance requirement, but rather as a controls framework that provides the opportunity to reduce risk to the organisation.

PricewaterhouseCoopers has developed a five-phase approach that enables PCI compliance through the identification and remediation of risk associated with payment card data. Our approach uses the PCI DSS as a baseline controls framework that is supplemented with leading risk management practices and our compliance and threat management experience.

- Phase 1: Data flow analysis
- Phase 2: Compliance gap analysis
- Phase 3: PCI remediation planning
- Phase 4: Remediation
- Phase 5: Operationalising compliance.

Once an organisation reaches initial compliance, the PCI program should be integrated within a broader governance, risk, and compliance framework to achieve greater efficiencies and further reduce risk.

## How can PricewaterhouseCoopers help?

PwC has extensive experience helping clients achieve PCI compliance in a cost-effective and risk-focused manner. We have been involved in the delivery of PCI-related services since 2004 and have delivered over 150,000 hours of professional services. We help our clients assess their environments, remediate their gaps, and operationalise their compliance programs. We also assist our clients with the design and implementation of solutions to reduce their PCI compliance scope, compliance costs, and operational costs, while increasing security and controls effectiveness.

For more information about our qualifications and service offerings, please contact Jan Schreuder or Charles Carmakal:



**Jan Schreuder**  
Partner  
P: +61 (2) 8266 1059  
E: jan.schreuder@au.pwc.com



**Charles Carmakal**  
Director  
P: +61 (2) 8266 0184  
E: charles.carmakal@au.pwc.com